In the United States Patent and Trademark Office

In re the application of: Banerjee et al.	)		
Filed: 10/31/2003	)	Group Art Unit:	2457
For: Host-based network intrusion detection systems	)	Examiner:	Ramy M. Osman
App. No. 10/698,197	)		
Appellant's Docket: JP920030162US1	)		

Mail Stop Appeal Brief - Patents
Commissioner of Patents and Trademarks
PO Box 1450
Alexandria, VA 22313-1450

This is an appeal from the Final Rejection of May 12, 2009 in which pending claims 1-4, 7, 9-11, 13-16, 19-23, 25-28, 31, 33-34, and 36-44 were rejected.

REAL PARTY IN INTEREST

The assignee, International Business Machines Corporation, is the real party in interest.

RELATED APPEALS AND INTERFERENCES

This is the first appeal in the present patent application. There are no other appeals or interferences known to the appellant or its legal representative. International Business Machines Corporation is the sole assignee of the patent application.

STATUS OF CLAIMS

Claims 1-4, 7, 9-11, 13-16, 19-23, 25-28, 31, 33-34, and 36-44 are pending in the application. Claims 5-6, 8, 17-18, 29-30, and 32 were previously canceled. Claims 12, 24, and 35 were previously withdrawn.

The claims appealed herein include claims 1, 2, 13, 14, 25, 26, 37, 40, and 43.

The original application, filed October 31, 2003, included claims 1-35.

An Office action of June 14, 2007, presented a restriction requirement with claims grouped as claims 1-11, 13-23, and 25-34 in Group I, and claims 12, 24, and 35 in Group II. In a Response to Restriction Requirement of July 6, 2007, Appellant elected to prosecute the claims in Group I, claims 1-11, 13-23, and 25-34, without traversal, wherein the claims of Group I were to be prosecuted alone (and the claims of Group II were to be correspondingly withdrawn).

In a nonfinal Office action of September 27, 2007, Examiner objected to claims 2, 14, 26 for minor informalities. Examiner also objected to claims 6-8 on grounds that they had improper dependency numbering.

In Reply A, filed December 27, 2007, Appellant responsively amended claims 2, 14 and 26 in accordance with Examiner's request. Appellant also responsively amended claim 1 to incorporate claims 6 and 8, canceled claims 6 and 8, and amended claim 7, thereby overcoming the objection.

A final Office of March 3, 2008, presented new grounds of rejection. Specifically, claims 1, 3-11,13,15-23, 25 and 27-34 were rejected under 35 U.S.C.

103(a) as being unpatentable over US Patent Publication No. 200310101353 ("Tarquini") in view of US Patent No. 7,185,368 ("Copeland"), or possibly US Patent No. 6,851,061 ("Holland "). (Copeland was recited in the broad statement of the rejections, but Holland was recited in the detailed remarks.) Claims 2, 14, and 26 were rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini in view Copeland, or possibly Holland. (Again, Copeland was recited in the broad statement of the rejections, but Holland was recited in the detailed remarks.) Claims 11, 23, and 34 were rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini in view of US Patent Publication No 200410117478 ("Triulzi").

In a Reply accompanying a Request for Continued Examination filed August 4, 2008, Appellant traversed the rejections and also submitted amendments to claims 1, 2, 7, 13, 14, 19, 20, 25, 26, and 31 and submitted new claims 36-44, merely to expedite allowance.

A non-final Office action of October 17, 2008, withdrew the rejection of claims 1-4, 7, 9-11,13-16, 19-23, 25-28, 31 and 33-34 but introduced new grounds of rejection, rejecting claims 1-4, 7, 9-11, 13-16, 19-23, 25-28, 31, 33, 34 and 36-44 under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061).

In a Reply to Nonfinal Office Action filed January 21, 2009, Appellant traversed the rejection of claims 1-4, 7, 9-11, 13-16, 19-23, 25-28, 31, 33, 34 and 36-44 under 35 U.S.C. 103(a) as being unpatentable over Yadav in view of Holland (US Patent No 6,851,061).

The present, final Office action of May 12, 2009 (the "present Office action"), repeats the prior rejection of claims 1-4,7,9- 11,13-16, 19-23, 25-28, 31 and 33-34 under 35 U.S.C. 103(a) as being unpatentable over Yadav in view of Holland (US Patent No 6,851,061).

Appellant appealed the rejection in a Notice of Appeal filed August 11, 2009.

STATUS OF AMENDMENTS

There are no amendments in connection with this appeal. All amendments that have been submitted have been entered. The claims in the Claim Appendix herein set out the claims that are the subject of the appeal.

SUMMARY OF CLAIMED SUBJECT MATTER

The present application discloses methods, systems, and computer program products for detecting and preventing an intrusion in a communications network.

Existing Network Intrusion Detection Systems (NIDS) are unsuitable for deployment on every host in a network due to problems that are inherent in the architecture of such NIDS. NIDS use promiscuous mode capture and analysis, which induces significant overhead on the system. NIDS are vulnerable to insertion and evasion attacks.

Intrusion signatures are often piecemeal. That is, a network intrusion can be camouflaged in different network packets that can cause a problem when coalesced. Intrusion detection between the transport and network layers does not detect signatures spread across packets, since the network layer doesn't have the ability or the knowledge to coalesce fragmented packets. Coalescing such fragmented packets is the job of the transport layer. The application layer needs to be presented information as a whole and not in the fragmented form in which the packets arrived. It is, therefore, evident that scanning is more effective according to the arrangement recited in the claims of the present application.

Claim 1

Claim 1, describes a computer-implemented method for detecting an intrusion in a communications network. The claim includes steps, as follows:

Step: accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network

protocol associated with said communications network to receive data packets for the application from the transport layer.

Step: scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process in a), wherein the data packets are directed to the application from a remote host via the communications network, and wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ.

Step: determining if said scanned data packets are malicious.

Step: taking at least one action to prevent the application from processing data packets from the remote host to the application responsive to c) determining that any of the scanned data packets are malicious.

The specification describes the method of claim 1 in terms of an embodiment of the invention. Specifically, regarding support for claim 1, see application as filed page 4, lines 15-18 (A method of detecting an intrusion in a communications network, the method comprising the steps of); Fig. 7, page 10, lines 12-16, page 11, lines 18-19 & 26-28 (accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system); page 5, line 12, page 9, lines 17-19, and page 10, lines 28-29 (wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer); page 5, lines 13-16 page 6, lines 6-8(scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process); Fig.'s 3, 5 & 6, page 5, lines 12-16 & 21-25, page 7, lines 23-27, page 9, lines 16-17, and page 10, lines 31-32 (wherein the data packets are directed to the application from a remote host via the communications network, and wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ); Fig.'s 5 & 6, page 11, lines 4-6 (determining if said scanned data packets are malicious); Fig. 7, page 11, lines 19-28

(taking at least one action to prevent the application from processing data packets from the remote host to the application responsive to c) determining that any of the scanned data packets are malicious).

Claim 2

Claim 2 depends upon method claim 1, wherein said at least one action includes terminating the application.

Regarding support for claim 2, see application as filed, Fig.'s 5, 6, & 7, page 11, lines 4-6 & 19-27 (wherein said at least one action includes terminating the application).

Claim 3

Claim 3 depends upon method claim 1, further comprising the step of transmitting to said application layer any data packets determined not to be malicious.

Regarding support for claim 3, see application as filed, Fig. 6, page 11, lines 12-13 (further comprising the step of transmitting to said application layer any data packets determined not to be malicious).

Claim 4

Claim 4 depends upon method claim 1, wherein said scanning and determining steps are implemented using a scan module.

Regarding support for claim 4, see application as filed, Fig.'s 1, 2, 9, & 10, page 7, lines 13-15, page 8, lines 9-10, page 10, lines 27-29, page 12, lines 20-22 & 30-31, & page 14, lines 27-28 (wherein said scanning and determining steps are implemented using a scan module).

Claim 7

Claim 7 depends upon method claim 1, further comprising the step of obtaining data from said at least one ARQ.

Regarding support for claim 7, see application as filed, Fig.'s 4 & 7, page 10, lines 15-16, page 11, lines 18-19 (further comprising the step of obtaining data from said at least one ARQ).

Claim 9

Claim 9 depends upon method claim 1, further comprising the step of dispatching said data packets to one or more handlers for scanning, if said protocol is monitored.

Regarding support for claim 9, see application as filed, Fig. 8, page 12, lines 1-3 (further comprising the step of dispatching said data packets to one or more handlers for scanning, if said protocol is monitored).

Claim 10

Claim 10 depends upon method claim 1, wherein said scanning and determining steps are implemented using a scan daemon.

Regarding support for claim 7, see application as filed, Fig. 7, page 11, lines 16-28 (wherein said scanning and determining steps are implemented using a scan daemon).

Claim 11

Claim 11 depends upon method claim 1, further comprising the step of the target computer system generating fake, network-accessible services.

Regarding support for claim 7, see application as filed, Fig. 10, page 6, lines 30-31, & page 12, line 29 – page 13, line 13 (further comprising the step of the target computer system generating fake, network-accessible services).

Claim 13

Claim 13, describes a computer system for detecting an intrusion originating from a remote host and communicated to the target computer system via a communications network. The target computer system includes a storage unit for storing data, instructions for a processing unit, and a processing unit coupled to said

storage unit. The processing unit is programmed to perform steps responsive to the instructions. The claim has steps as follows:

Step: accessing, by a network intrusion detection process of the target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer;

Step: scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process in a), wherein the data packets are directed to the application from the remote host via the communications network, and wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ;

Step: determining if said scanned data packets are malicious; and

Step: taking at least one action to prevent the application from processing the data packets from the remote host to the application responsive to c) determining that any of the scanned data packets are malicious.

The specification describes the computer system of claim 13 in terms of an embodiment of the invention. Specifically, regarding support for claim 13, see application as filed page 14, lines 9-28 (A target computer system for detecting an intrusion originating from a remote host and communicated to the target computer system via a communications network, the target computer system comprising a storage unit for storing data and instructions for a processing unit; and a processing unit coupled to said storage unit, said processing unit being programmed to perform steps responsive to the instructions); Fig. 7, page 10, lines 12-16, page 11, lines 18-19 & 26-28 (accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system); page 5, line 12, page 9, lines 17-19, and page 10, lines 28-29 (wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said

communications network to receive data packets for the application from the transport layer); page 5, lines 13-16 page 6, lines 6-8(scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process); Fig.'s 3, 5 & 6, page 5, lines 12-16 & 21-25, page 7, lines 23-27, page 9, lines 16-17, and page 10, lines 31-32 (wherein the data packets are directed to the application from a remote host via the communications network, and wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ); Fig.'s 5 & 6, page 11, lines 4-6 (determining if said scanned data packets are malicious); Fig. 7, page 11, lines 19-28 (taking at least one action to prevent the application from processing data packets from the remote host to the application responsive to c) determining that any of the scanned data packets are malicious).

Claim 14

Claim 14 depends upon system claim 13, wherein said at least one action includes terminating the application.

Regarding support for claim 14, see application as filed, Fig.'s 5, 6, & 7, page 11, lines 4-6 & 19-27 (wherein said at least one action includes terminating the application).

Claim 15

Claim 15 depends upon system claim 13, further comprising the step of transmitting to said application layer any data packets determined not to be malicious.

Regarding support for claim 15, see application as filed, Fig. 6, page 11, lines 12-13 (further comprising the step of transmitting to said application layer any data packets determined not to be malicious).

Claim 16

Claim 16 depends upon system claim 13, wherein said scanning and determining steps are implemented using a scan module.

Regarding support for claim 16, see application as filed, Fig.'s 1, 2, 9, & 10, page 7, lines 13-15, page 8, lines 9-10, page 10, lines 27-29, page 12, lines 20-22 & 30-31, & page 14, lines 27-28 (wherein said scanning and determining steps are implemented using a scan module).

Claim 19

Claim 19 depends upon system claim 13, wherein said processing unit is programmed to obtain data form said at least one ARQ.

Regarding support for claim 19, see application as filed, Fig.'s 4 & 7, page 10, lines 15-16, page 11, lines 18-19 (wherein said processing unit is programmed to obtain data form said at least one ARQ).

Claim 20

Claim 20 depends upon system claim 13, wherein said scanning is performed on data packets from said at least one ARQ.

Regarding support for claim 19, see application as filed, Fig.'s 4 & 7, page 10, lines 15-16, page 11, lines 18-19 (wherein said scanning is performed on data packets from said at least one ARQ).

Claim 21

Claim 21 depends upon system claim 13, wherein said processing unit is programmed to dispatch said data packets to one or more handlers for scanning, if said protocol is monitored.

Regarding support for claim 21, see application as filed, Fig. 8, page 12, lines 1-3 (further wherein said processing unit is programmed to dispatch said data packets to one or more handlers for scanning, if said protocol is monitored).

Claim 22

Claim 22 depends upon system claim 13, wherein said scanning and determining steps are implemented using a scan daemon.

Regarding support for claim 13, see application as filed, Fig. 7, page 11, lines 16-28 (wherein said scanning and determining steps are implemented using a scan daemon).

Claim 23

Claim 23 depends upon system claim 13, wherein said processing unit is programmed to generate fake, network-accessible services.

Regarding support for claim 23, see application as filed, Fig. 10, page 6, lines 30-31, & page 12, line 29 – page 13, line 13 (wherein said processing unit is programmed to generate fake, network-accessible services)..

Claim 25

Claim 25, describes a computer program product stored on a computer-readable storage medium, the computer program product having instructions for execution by a computer, wherein the instructions, when executed by the computer, cause the computer to implement a method comprising the following steps:

Step: accessing, by a network intrusion detection process of the target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer;

Step: scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process in a), wherein the data packets are directed to the application from the remote host via the communications network, and wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ;

Step: determining if said scanned data packets are malicious; and

Step: taking at least one action to prevent the application from processing the data packets from the remote host to the application responsive to c) determining that any of the scanned data packets are malicious.

The specification describes the computer program product of claim 25 in terms of an embodiment of the invention. Specifically, regarding support for claim 25, see application as filed page 13, line 19 – page 14, line 6 (A computer program product stored on a computer-readable storage medium, the computer program product having instructions for execution by a computer, wherein the instructions, when executed by the computer, cause the computer to implement a method comprising the steps of); Fig. 7, page 10, lines 12-16, page 11, lines 18-19 & 26-28 (accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system); page 5, line 12, page 9, lines 17-19, and page 10, lines 28-29 (wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer); page 5, lines 13-16 page 6, lines 6-8(scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process); Fig.'s 3, 5 & 6, page 5, lines 12-16 & 21-25, page 7, lines 23-27, page 9, lines 16-17, and page 10, lines 31-32 (wherein the data packets are directed to the application from a remote host via the communications network, and wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ); Fig.'s 5 & 6, page 11, lines 4-6 (determining if said scanned data packets are malicious); Fig. 7, page 11, lines 19-28 (taking at least one action to prevent the application from processing data packets from the remote host to the application responsive to c) determining that any of the scanned data packets are malicious).

Claim 26

Claim 26 depends upon computer program product claim 25, wherein said at least one action includes terminating the application.

Regarding support for claim 26, see application as filed, Fig.'s 5, 6, & 7, page 11, lines 4-6 & 19-27 (wherein said at least one action includes terminating the application).

Claim 27

Claim 27 depends upon computer program product claim 25, further comprising transmitting to said application layer any data packets determined not to be malicious.

Regarding support for claim 27, see application as filed, Fig. 6, page 11, lines 12-13 (further comprising transmitting to said application layer any data packets determined not to be malicious).

Claim 28

Claim 28 depends upon computer program product claim 25, wherein said scanning and determining are implemented using a scan module.

Regarding support for claim 28, see application as filed, Fig.'s 1, 2, 9, & 10, page 7, lines 13-15, page 8, lines 9-10, page 10, lines 27-29, page 12, lines 20-22 & 30-31, & page 14, lines 27-28 (wherein said scanning and determining are implemented using a scan module).

Claim 31

Claim 31 depends upon computer program product claim 25, the steps further comprising obtaining data from said at least one ARQ.

Regarding support for claim 31, see application as filed, Fig.'s 4 & 7, page 10, lines 15-16, page 11, lines 18-19 (the steps further comprising obtaining data from said at least one ARQ).

Claim 33

Claim 33 depends upon computer program product claim 25, the steps further comprising dispatching said data packets to one or more handlers for scanning, if said protocol is monitored.

Regarding support for claim 33, see application as filed, Fig. 8, page 12, lines 1-3 (the steps further comprising dispatching said data packets to one or more handlers for scanning, if said protocol is monitored).

Claim 34

Claim 34 depends upon computer program product claim 25, wherein said scanning and determining steps are implemented using a scan daemon.

Regarding support for claim 34, see application as filed, Fig. 7, page 11, lines 16-28 (wherein said scanning and determining steps are implemented using a scan daemon).

Claim 36

Claim 36 depends upon method claim 1, wherein said at least one action includes modifying firewall rules to prevent reception of data packets from the host computer system.

Regarding support for claim 36, see application as filed, Fig. 3, page 10, lines 4-6 (wherein said at least one action includes modifying firewall rules to prevent reception of data packets from the host computer system).

Claim 37

Claim 37 depends upon method claim 1, wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and wherein said at least one action includes intimating the transport layer to tear down the remote host connection.

Regarding support for claim 37, see application as filed, Fig. 3, page 10, lines 1-5 (wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and

wherein said at least one action includes intimating the transport layer to tear down the remote host connection).

Claim 38

Claim 38 depends upon method claim 37, wherein after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection.

Regarding support for claim 38, see application as filed, Fig. 7, page 11, lines 16-28 (wherein after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection).

Claim 39

Claim 39 depends upon system claim 13, wherein said at least one action includes modifying firewall rules to prevent reception of data packets from the host computer system.

Regarding support for claim 39, see application as filed, Fig. 3, page 10, lines 4-6 (wherein said at least one action includes modifying firewall rules to prevent reception of data packets from the host computer system).

Claim 40

Claim 40 depends upon system claim 13, wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and wherein said at least one action includes intimating the transport layer to tear down the remote host connection.

Regarding support for claim 40, see application as filed, Fig. 3, page 10, lines 1-5 (wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and wherein said at least one action includes intimating the transport layer to tear down the remote host connection).

Claim 41

Claim 41 depends upon system claim 40, wherein after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection.

Regarding support for claim 38, see application as filed, Fig. 7, page 11, lines 16-28 (wherein after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection).

Claim 42

Claim 42 depends upon computer program product claim 25, wherein said at least one action includes modifying firewall rules to prevent reception of data packets from the host computer system.

Regarding support for claim 39, see application as filed, Fig. 3, page 10, lines 4-6 (wherein said at least one action includes modifying firewall rules to prevent reception of data packets from the host computer system).

Claim 43

Claim 43 depends upon computer program product claim 25, wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and wherein said at least one action includes intimating the transport layer to tear down the remote host connection.

Regarding support for claim 43, see application as filed, Fig. 3, page 10, lines 1-5 (wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and wherein said at least one action includes intimating the transport layer to tear down the remote host connection).

Claim 44

Claim depends upon computer program product claim 43, wherein after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection.

Regarding support for claim 44, see application as filed, Fig. 7, page 11, lines 16-28 (wherein after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Is the rejection in the Final Office Action proper, wherein claims 1-4, 7, 9-11, 13-16, 19-23, 25-28, 31, 33, 34 and 36-44 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061)?

ARGUMENTS

1. Rejection Under 35 U.S.C. 103(a)

Claim 1

Claim 1 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061). Appellant respectfully submits that the rejection is improper.

Examiner's Position

Appellant's arguments filed 1/21/09 have been fully considered but are not persuasive. Appellant argues that Yadav fails to teach the "scanning of packets that have been processed by the transport layer and are on their way to a particular application queue receive" as mentioned in bottom of page 11 of remarks. In reply, Appellant is reminded that the claim language is broad and is thus given its broadest reasonable interpretation. Since the claim only passingly and broadly mentions a "communication to an application receive queue" then this is treated broadly since the claim fails to limit whether this communication is destined to, belongs to, coming from, etc. in regards to the queue. There is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant's Rebuttal

The Present Office Action maintains the same prior art rejection stated in the previous Office action, which was dated October 17, 2008, and which asserted that Yadav, column 5, lines 14-32, teaches "a method of detecting an intrusion in a communications network, the method comprising the steps of: a) accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer;" and that Yadav, column 6, lines 17-37, teaches "b) scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process in a), wherein the data packets are directed to the application from a remote host via the communications network, and wherein the scanning is after the data packets have been processed by the e-transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ," as recited by claim 1 in the present application. Appellant respectfully disagrees for at least the following reasons.

Yadav teaches the use of an intrusion detection system 230 between a network driver and a transport layer. Yadav, col. 5, lines 1-4. Yadav states that IDS 230 may also have "additional components 232 placed elsewhere in the network stack." Yadav, col. 5, lines 7-8. Yadav goes on to state that "application-level detection may be implemented in one or more components placed just below and/or just inside the application layer 220." Yadav, col. 5, lines 10-13. (Yadav explains that this can be done by an application-level component 234 and/or individual application-level components 236 for respective applications. Yadav, col. 5, lines 14-15 and 25-26.)

However, Yadav makes it clear that these "one or more components placed just below and/or just inside the application layer 220" are in addition to IDS 230. See 5, lines 14-15 (stating that component 234 is "part of" IDS 230); see also Yadav, col. 5, lines 25-26 (stating that components 236 may be in addition to component

234); see also Yadav, col. 5, lines 25-26 (stating that components 236 may be an alternative to component 234, and not stating that component 234 is an alternative to 230). That is, Yadav teaches that IDS 230 performs a firewall function that includes monitoring network traffic to block traffic that is a prelude to intrusion. Yadav, col. 5, lines 42-53. Nowhere does Yadav teach or suggest that application-level components 234 or 236 perform the monitoring and blocking. And nowhere does Yadav teach or suggest that the basic IDS 230 is located somewhere other than between the network driver and the transport layer.

Thus, it should be appreciated from the above that in connection with intrusion detection system 230 and application-level components 234 and 236, Yadav does not teach or suggest scanning of packets that have been processed by the transport layer and are on their way to a particular application receive queue, which is more particularly pointed out in claim 1 of the present case as "a) accessing . . . communication to an application receive queue (ARQ) . . . , wherein the ARQ functions intermediate the application layer and a transport layer . . . to receive data packets for the application from the transport layer" and "scanning for the application . . . only the data packets accessed by the network intrusion detection process in a), . . . wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

That Yadav does not teach or suggest what is claimed in the present case is made all the more clear by analysis of teaching by Yadav in connection with Fig's 2B, 3 and 4 at col. 5, line 35 – col. 8, line 33. That is, Yadav teaches that a structure illustrated in FIG. 2B includes a network traffic enforcer 282, which, like IDS 230 of FIG. 2A, is shown below a transport layer. Further, Yadav's FIG. 2B illustrates an application rule enforcer 284 below an application layer, like application level component 234 of FIG. 2A. In the description of the processes illustrated in Fig's 3 and 4, Yadav makes more clear how the component below the application layer communicates with the component below the transport layer, and explains how the lower component monitors and blocks. From this explanation, it is clear that what Yadav teaches is very different than the scanning claimed in the present case.

In particular, Yadav teaches that application rule enforcer 284 handles an outgoing network service request from an application. Yadav, col. 7, lines 53-60. If the request is within the permitted policy, application rule enforcer 284 signals network traffic enforcer 282 to open a "channel" for the application, for which Yadav describes an example. Yadav, col. 7, lines 53-60 (describing how channel is defined by application rule enforcer specifying a channel protocol, source and destination IP addresses and source and destination ports). Network traffic enforcer 282 responsively opens the channel and adds it to an authorization list 405. Yadav, col. 8, lines 21-24.

Further, "The network traffic enforcer 282 monitors incoming network traffic. If an inbound communication 262 fails to correspond to an authorized request (i.e., the inbound communication was not effectively pre-approved by the application rule enforcer), the communication is dropped (i.e., blocked from passage to another layer in the network stack.)." Yadav, col. 6, lines 26-31. Yadav does not explicitly state how network traffic enforcer 282 determines that an inbound communication 262 fails to correspond to an authorized request. But it would be logical and consistent, in view of what Yadav *does* explicitly teach, for this to be done by matching an authorized channel on the authorization list 405 with a "channel" indicated by inbound communication 262. This would, of course, be done *below* the transport layer, since it would be done by the network traffic enforcer 282. See Yadav, col. 6, lines 26-31 ("The network traffic enforcer 282 monitors incoming network traffic. If an inbound communication 262 fails to correspond to an authorized request . . . the communication is . . . blocked from passage to another layer . . .").

Thus, it should be appreciated even more particularly from the above that in connection with network traffic enforcer 282 and application rule enforcer 284, Yadav does not teach or suggest "a) accessing . . . communication to an application receive queue (ARQ) . . . , wherein the ARQ functions intermediate the application layer and a transport layer . . . to receive data packets for the application from the transport layer" and "scanning for the application . . . only the data packets accessed by the network intrusion detection process in a), . . . wherein the scanning is after the data

packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

The Present Office Action discounts Appellant's arguments presented above, which were also presented in Appellant's reply of January 21, 2009. Specifically, the Present Office Action responds that claim 1, for example, "only passingly and broadly mentions . . . 'communication to an application receive queue.'" Applicant respectfully submits that this mischaracterizes the claim.

Further, Appellant pointed out specific language in the claim in the January 21, 2009, reply that relates to this matter. See above remarks and similar remarks in Appellant's reply of January 21, 2009, beginning at the end of page 11, which in addition to pointing out that claim 1 recites "communication to an application receive queue," also points out much more that the claim recites with regard to the ARQ. In particular, Appellant has pointed out the claim recites that the application receive queue ("ARQ") "functions intermediate the application layer and a transport layer." Appellant also pointed out that included in the ARQ functioning is functioning "to receive data packets for the application from the transport layer." Appellant also pointed out that the claimed method recites "scanning for the application . . . only the data packets accessed by the network intrusion detection process in a). " This makes clear that the claim limits the scanning to only data packets accessed by the network intrusion detection process in "communication to an application receive queue (ARQ) . . . intermediate the application layer and . . . transport layer . . . to receive data packets for the application from the transport layer." Still further, Appellant pointed out that the claim states "the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

Thus, Appellant respectfully disagrees with the assertion in the Present Office Action that the claim only passingly and broadly mentions "communication to an application receive queue," and submits that the Present Office Action essentially ignores the claim language recited above and Appellant's explanation thereof.

Further, the Present Office Action states "There Is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is

noted that the features upon which Appellant relies are not recited in the rejected claims." Again, Appellant respectfully submits that this mischaracterizes the claim and ignores specific claim language about communication processed by a transport layer and then passed to an application receive queue between the transport layer and the application layer. That is, as Appellant has pointed out, the claimed method recites "scanning for the application . . . only the data packets accessed by the network intrusion detection process in a). " This makes clear that the claim limits the scanning to only data packets accessed by the network intrusion detection process in "communication to an application receive queue (ARQ) . . . intermediate the application layer and . . . transport layer . . . to receive data packets for the application from the transport layer," since a) states "communication to an application receive queue (ARQ) . . . intermediate the application layer and . . . transport layer . . . to receive data packets for the application from the transport layer." Still further, Appellant pointed out that the claim limits the scanning to being "after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

The other art relied upon in the rejection does not cure the above deficiencies.

For all the above reasons, Appellant respectfully submits that claim 1 is patentably distinct.

Claim 2

Claim 2 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061). Appellant respectfully submits that the rejection is improper.

Examiner's Position

Appellant's arguments filed 1/21/09 have been fully considered but they are not persuasive. Appellant argues that Yadav fails to teach the "scanning of packets that have been processed by the transport layer and are on their way to a particular application queue receive" as mentioned in bottom of pg 11 of remarks. In reply, Appellant is reminded that the claim language is broad and is thus given its broadest reasonable interpretation. Since the claim only passingly and broadly mentions a "communication to an application receive queue" then this is treated broadly since the claim fails to limit whether this communication is destined to, belongs to, coming from, etc. in regards to the queue. There is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant's Rebuttal

The Present Office Action maintains the same prior art rejection stated in the previous Office action, which was dated October 17, 2008, and which asserted that Yadav column 5, lines 47-52, teaches tracking abnormally behaving applications. The previous Office action stated that "it is common knowledge that if an application is behaving abnormally, and that it is possible due to an intrusion, then that application should be terminated in order to prevent any harmful effects that may result from the intrusion" and that it would have been obvious for one of ordinary skill in the art to modify Yadav to include terminating the application responsive to determining a scanned data packet is malicious, in order to prevent any harmful

effects that may result from the intrusion. Appellant respectfully submits that this analysis is not relevant to the present invention, as claimed.

In the present case, intrusions are detected before data received from a remote host for an application has been passed to the application, and thus before the data can cause the application to behave abnormally by scanning data for an application in the manner recited in claim 1. See previous explanation on page 13 of Appellant's Response Accompanying Request for Continuing Examination, submitted August 4, 2008. Nevertheless, in one aspect of the present invention, as recited in claim 2 when read in connection with claim 1, an application is terminated responsive to detecting the malicious data packet. It logically follows from claim 1 and 2 of the present case that an application is terminated due to detecting an intrusion, but before the application can be subjected to any harmful effects of the intrusion and, therefore, before the application has an opportunity to behave abnormally. This does not follow from the logic presented in the previous Office action that posits reasons for terminating an application if the application is behaving abnormally due to an intrusion. Therefore, it would not be obvious to modify Yadav according to the logic put forward by the previous Office action (which is not further supplemented in the Present Office Action).

The other art relied upon in the rejection does not cure the above deficiencies.

Consequently, Appellant respectfully submits that claim 2 is patentably distinct.

Further, Appellant presented arguments contrary to the alleged common knowledge presented in the previous Office action and requested in the reply of January 21, 2009, in accordance with MPEP 2144.03(C), that Examiner submit an examiner's affidavit or declaration providing a basis for the alleged common knowledge if the rejection of claim 2 was maintained. However, the rejection was maintained but no examiner's affidavit or declaration has been provided by the Present Office Action. For this additional reason Appellant respectfully submits that claim 2 is patentably distinct.

Claim 13

Claim 13 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061). Appellant respectfully submits that the rejection is improper.

Examiner's Position

Appellant's arguments filed 1/21/09 have been fully considered but are not persuasive. Appellant argues that Yadav fails to teach the "scanning of packets that have been processed by the transport layer and are on their way to a particular application queue receive" as mentioned in bottom of page 11 of remarks. In reply, Appellant is reminded that the claim language is broad and is thus given its broadest reasonable interpretation. Since the claim only passingly and broadly mentions a "communication to an application receive queue" then this is treated broadly since the claim fails to limit whether this communication is destined to, belongs to, coming from, etc. in regards to the queue. There is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant's Rebuttal

The Present Office Action maintains the same prior art rejection stated in the previous Office action, which was dated October 17, 2008, and which asserted that Yadav, column 5, lines 14-32, teaches "detecting an intrusion in a communications network," which includes "a) accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the

application from the transport layer." The Present Office action also asserts that Yadav, column 6, lines 17-37, teaches "b) scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process in a), wherein the data packets are directed to the application from a remote host via the communications network, and wherein the scanning is after the data packets have been processed by the e-transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ," as recited by claim 13 in the present application. Appellant respectfully disagrees for at least the following reasons.

Yadav teaches the use of an intrusion detection system 230 between a network driver and a transport layer. Yadav, col. 5, lines 1-4. Yadav states that IDS 230 may also have "additional components 232 placed elsewhere in the network stack." Yadav, col. 5, lines 7-8. Yadav goes on to state that "application-level detection may be implemented in one or more components placed just below and/or just inside the application layer 220." Yadav, col. 5, lines 10-13. (Yadav explains that this can be done by an application-level component 234 and/or individual application-level components 236 for respective applications. Yadav, col. 5, lines 14-15 and 25-26.)

However, Yadav makes it clear that these "one or more components placed just below and/or just inside the application layer 220" are in addition to IDS 230. See 5, lines 14-15 (stating that component 234 is "part of" IDS 230); see also Yadav, col. 5, lines 25-26 (stating that components 236 may be in addition to component 234); see also Yadav, col. 5, lines 25-26 (stating that components 236 may be an alternative to component 234, and not stating that component 234 is an alternative to 230). That is, Yadav teaches that IDS 230 performs a firewall function that includes monitoring network traffic to block traffic that is a prelude to intrusion. Yadav, col. 5, lines 42-53. Nowhere does Yadav teach or suggest that application-level components 234 or 236 perform the monitoring and blocking. And nowhere does Yadav teach or suggest that the basic IDS 230 is located somewhere other than between the network driver and the transport layer.

Thus, it should be appreciated from the above that in connection with intrusion detection system 230 and application-level components 234 and 236, Yadav does not teach or suggest scanning of packets that have been processed by the transport layer and are on their way to a particular application receive queue, which is more particularly pointed out in claim 13 of the present case as "a) accessing . . . communication to an application receive queue (ARQ) . . . , wherein the ARQ functions intermediate the application layer and a transport layer . . . to receive data packets for the application from the transport layer" and "scanning for the application . . . only the data packets accessed by the network intrusion detection process in a), . . . wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

That Yadav does not teach or suggest what is claimed in the present case is made all the more clear by analysis of teaching by Yadav in connection with Fig's 2B, 3 and 4 at col. 5, line 35 – col. 8, line 33. That is, Yadav teaches that a structure illustrated in FIG. 2B includes a network traffic enforcer 282, which, like IDS 230 of FIG. 2A, is shown below a transport layer. Further, Yadav's FIG. 2B illustrates an application rule enforcer 284 below an application layer, like application level component 234 of FIG. 2A. In the description of the processes illustrated in Fig's 3 and 4, Yadav makes more clear how the component below the application layer communicates with the component below the transport layer, and explains how the lower component monitors and blocks. From this explanation, it is clear that what Yadav teaches is very different than the scanning claimed in the present case.

In particular, Yadav teaches that application rule enforcer 284 handles an outgoing network service request from an application. Yadav, col. 7, lines 53-60. If the request is within the permitted policy, application rule enforcer 284 signals network traffic enforcer 282 to open a "channel" for the application, for which Yadav describes an example. Yadav, col. 7, lines 53-60 (describing how channel is defined by application rule enforcer specifying a channel protocol, source and destination IP addresses and source and destination ports). Network traffic enforcer 282

responsively opens the channel and adds it to an authorization list 405. Yadav, col. 8, lines 21-24.

Further, "The network traffic enforcer 282 monitors incoming network traffic. If an inbound communication 262 fails to correspond to an authorized request (i.e., the inbound communication was not effectively pre-approved by the application rule enforcer), the communication is dropped (i.e., blocked from passage to another layer in the network stack.)." Yadav, col. 6, lines 26-31. Yadav does not explicitly state how network traffic enforcer 282 determines that an inbound communication 262 fails to correspond to an authorized request. But it would be logical and consistent, in view of what Yadav *does* explicitly teach, for this to be done by matching an authorized channel on the authorization list 405 with a "channel" indicated by inbound communication 262. This would, of course, be done *below* the transport layer, since it would be done by the network traffic enforcer 282. See Yadav, col. 6, lines 26-31 ("The network traffic enforcer 282 monitors incoming network traffic. If an inbound communication 262 fails to correspond to an authorized request . . . the communication is . . . blocked from passage to another layer . . .").

Thus, it should be appreciated even more particularly from the above that in connection with network traffic enforcer 282 and application rule enforcer 284, Yadav does not teach or suggest "a) accessing . . . communication to an application receive queue (ARQ) . . . , wherein the ARQ functions intermediate the application layer and a transport layer . . . to receive data packets for the application from the transport layer" and "scanning for the application . . . only the data packets accessed by the network intrusion detection process in a), . . . wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

The Present Office Action discounts Appellant's arguments presented above, which were also presented in Appellant's reply of January 21, 2009. Specifically, the Present Office Action responds that claim 13 "only passingly and broadly mentions . . . 'communication to an application receive queue.'" Applicant respectfully submits that this mischaracterizes the claim.

Further, Appellant pointed out specific language in the claim in the January 21, 2009, reply that relates to this matter. See above remarks and similar remarks in Appellant's reply of January 21, 2009, beginning at the end of page 11, which in addition to pointing out that claim 1 (and, correspondingly, independent claims 13 and 25) recites "communication to an application receive queue," also points out much more that the claim recites with regard to the ARQ. In particular, Appellant has pointed out the claim recites that the application receive queue ("ARQ") "functions intermediate the application layer and a transport layer." Appellant also pointed out that included in the ARQ functioning is functioning "to receive data packets for the application from the transport layer." Appellant also pointed out that the claimed method recites "scanning for the application . . . only the data packets accessed by the network intrusion detection process in a). " This makes clear that the claim limits the scanning to only data packets accessed by the network intrusion detection process in "communication to an application receive queue (ARQ) . . . intermediate the application layer and . . . transport layer . . . to receive data packets for the application from the transport layer." Still further, Appellant pointed out that the claim states "the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

Thus, Appellant respectfully disagrees with the assertion in the Present Office Action that the claim only passingly and broadly mentions "communication to an application receive queue," and submits that the Present Office Action essentially ignores the claim language recited above and Appellant's explanation thereof.

Further, the Present Office Action states "There Is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claims." Again, Appellant respectfully submits that this mischaracterizes the claim and ignores specific claim language about communication processed by a transport layer and then passed to an application receive queue between the transport layer and the application layer. That is, as Appellant has pointed out, the claim recites "scanning for the application . . . only the data packets accessed by the network

intrusion detection process in a). " This makes clear that the claim limits the scanning to only data packets accessed by the network intrusion detection process in "communication to an application receive queue (ARQ) . . . intermediate the application layer and . . . transport layer . . . to receive data packets for the application from the transport layer," since a) states "communication to an application receive queue (ARQ) . . . intermediate the application layer and . . . transport layer . . . to receive data packets for the application from the transport layer." Still further, Appellant pointed out that the claim limits the scanning to being "after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

The other art relied upon in the rejection does not cure the above deficiencies.

For all the above reasons, Appellant respectfully submits that claim 13 is patentably distinct.

Claim 14

Claim 14 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061). Appellant respectfully submits that the rejection is improper.

Examiner's Position

Appellant's arguments filed 1/21/09 have been fully considered but they are not persuasive. Appellant argues that Yadav fails to teach the "scanning of packets that have been processed by the transport layer and are on their way to a particular application queue receive" as mentioned in bottom of pg 11 of remarks. In reply, Appellant is reminded that the claim language is broad and is thus given its broadest reasonable interpretation. Since the claim only passingly and broadly mentions a "communication to an application receive queue" then this is treated broadly since the claim fails to limit whether this communication is destined to, belongs to, coming from, etc. in regards to the queue. There is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant's Rebuttal

The Present Office Action maintains the same prior art rejection stated in the previous Office action, which was dated October 17, 2008, and which asserted that Yadav column 5, lines 47-52, teaches tracking abnormally behaving applications. The previous Office action stated that "it is common knowledge that if an application is behaving abnormally, and that it is possible due to an intrusion, then that application should be terminated in order to prevent any harmful effects that may result from the intrusion" and that it would have been obvious for one of ordinary skill in the art to modify Yadav to include terminating the application responsive to determining a scanned data packet is malicious, in order to prevent any harmful

effects that may result from the intrusion. Appellant respectfully submits that this analysis is not relevant to the present invention, as claimed.

In the present case, intrusions are detected before data received from a remote host for an application has been passed to the application, and thus before the data can cause the application to behave abnormally by scanning data for an application in the manner recited in claim 13. See previous explanation on page 13 of Appellant's Response Accompanying Request for Continuing Examination, submitted August 4, 2008. Nevertheless, in one aspect of the present invention, as recited in claim 14 when read in connection with claim 13, an application is terminated responsive to detecting the malicious data packet. It logically follows from claims 13 and 14 of the present case that an application is terminated due to detecting an intrusion, but before the application can be subjected to any harmful effects of the intrusion and, therefore, before the application has an opportunity to behave abnormally. This does not follow from the logic presented in the previous Office action that posits reasons for terminating an application if the application is behaving abnormally due to an intrusion. Therefore, it would not be obvious to modify Yadav according to the logic put forward by the previous Office action (which is not further supplemented in the Present Office Action).

The other art relied upon in the rejection does not cure the above deficiencies.

Consequently, Appellant respectfully submits that claim 14 is patentably distinct.

Further, Appellant presented arguments contrary to the alleged common knowledge presented in the previous Office action and requested in the reply of January 21, 2009, in accordance with MPEP 2144.03(C), that Examiner submit an examiner's affidavit or declaration providing a basis for the alleged common knowledge if the rejection of claim 14 was maintained. However, the rejection was maintained but no examiner's affidavit or declaration has been provided by the Present Office Action. For this additional reason Appellant respectfully submits that claim 14 is patentably distinct.

Claim 25

Claim 25 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061). Appellant respectfully submits that the rejection is improper.

Examiner's Position

Appellant's arguments filed 1/21/09 have been fully considered but are not persuasive. Appellant argues that Yadav fails to teach the "scanning of packets that have been processed by the transport layer and are on their way to a particular application queue receive" as mentioned in bottom of page 11 of remarks. In reply, Appellant is reminded that the claim language is broad and is thus given its broadest reasonable interpretation. Since the claim only passingly and broadly mentions a "communication to an application receive queue" then this is treated broadly since the claim fails to limit whether this communication is destined to, belongs to, coming from, etc. in regards to the queue. There is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant's Rebuttal

The Present Office Action maintains the same prior art rejection stated in the previous Office action, which was dated October 17, 2008, and which asserted that Yadav, column 5, lines 14-32, teaches "detecting an intrusion in a communications network," which includes "a) accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the

application from the transport layer." The Present Office Action also asserts that Yadav, column 6, lines 17-37, teaches "b) scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process in a), wherein the data packets are directed to the application from a remote host via the communications network, and wherein the scanning is after the data packets have been processed by the e-transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ," as recited by claim 25 in the present application. Appellant respectfully disagrees for at least the following reasons.

Yadav teaches the use of an intrusion detection system 230 between a network driver and a transport layer. Yadav, col. 5, lines 1-4. Yadav states that IDS 230 may also have "additional components 232 placed elsewhere in the network stack." Yadav, col. 5, lines 7-8. Yadav goes on to state that "application-level detection may be implemented in one or more components placed just below and/or just inside the application layer 220." Yadav, col. 5, lines 10-13. (Yadav explains that this can be done by an application-level component 234 and/or individual application-level components 236 for respective applications. Yadav, col. 5, lines 14-15 and 25-26.)

However, Yadav makes it clear that these "one or more components placed just below and/or just inside the application layer 220" are in addition to IDS 230. See 5, lines 14-15 (stating that component 234 is "part of" IDS 230); see also Yadav, col. 5, lines 25-26 (stating that components 236 may be in addition to component 234); see also Yadav, col. 5, lines 25-26 (stating that components 236 may be an alternative to component 234, and not stating that component 234 is an alternative to 230). That is, Yadav teaches that IDS 230 performs a firewall function that includes monitoring network traffic to block traffic that is a prelude to intrusion. Yadav, col. 5, lines 42-53. Nowhere does Yadav teach or suggest that application-level components 234 or 236 perform the monitoring and blocking. And nowhere does Yadav teach or suggest that the basic IDS 230 is located somewhere other than between the network driver and the transport layer.

Thus, it should be appreciated from the above that in connection with intrusion detection system 230 and application-level components 234 and 236, Yadav does not teach or suggest scanning of packets that have been processed by the transport layer and are on their way to a particular application receive queue, which is more particularly pointed out in claim 25 of the present case as "a) accessing . . . communication to an application receive queue (ARQ) . . . , wherein the ARQ functions intermediate the application layer and a transport layer . . . to receive data packets for the application from the transport layer" and "scanning for the application . . . only the data packets accessed by the network intrusion detection process in a), . . . wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

That Yadav does not teach or suggest what is claimed in the present case is made all the more clear by analysis of teaching by Yadav in connection with Fig's 2B, 3 and 4 at col. 5, line 35 – col. 8, line 33. That is, Yadav teaches that a structure illustrated in FIG. 2B includes a network traffic enforcer 282, which, like IDS 230 of FIG. 2A, is shown below a transport layer. Further, Yadav's FIG. 2B illustrates an application rule enforcer 284 below an application layer, like application level component 234 of FIG. 2A. In the description of the processes illustrated in Fig's 3 and 4, Yadav makes more clear how the component below the application layer communicates with the component below the transport layer, and explains how the lower component monitors and blocks. From this explanation, it is clear that what Yadav teaches is very different than the scanning claimed in the present case.

In particular, Yadav teaches that application rule enforcer 284 handles an outgoing network service request from an application. Yadav, col. 7, lines 53-60. If the request is within the permitted policy, application rule enforcer 284 signals network traffic enforcer 282 to open a "channel" for the application, for which Yadav describes an example. Yadav, col. 7, lines 53-60 (describing how channel is defined by application rule enforcer specifying a channel protocol, source and destination IP addresses and source and destination ports). Network traffic enforcer 282

responsively opens the channel and adds it to an authorization list 405. Yadav, col. 8, lines 21-24.

Further, "The network traffic enforcer 282 monitors incoming network traffic. If an inbound communication 262 fails to correspond to an authorized request (i.e., the inbound communication was not effectively pre-approved by the application rule enforcer), the communication is dropped (i.e., blocked from passage to another layer in the network stack.)." Yadav, col. 6, lines 26-31. Yadav does not explicitly state how network traffic enforcer 282 determines that an inbound communication 262 fails to correspond to an authorized request. But it would be logical and consistent, in view of what Yadav *does* explicitly teach, for this to be done by matching an authorized channel on the authorization list 405 with a "channel" indicated by inbound communication 262. This would, of course, be done *below* the transport layer, since it would be done by the network traffic enforcer 282. See Yadav, col. 6, lines 26-31 ("The network traffic enforcer 282 monitors incoming network traffic. If an inbound communication 262 fails to correspond to an authorized request . . . the communication is . . . blocked from passage to another layer . . .").

Thus, it should be appreciated even more particularly from the above that in connection with network traffic enforcer 282 and application rule enforcer 284, Yadav does not teach or suggest "a) accessing . . . communication to an application receive queue (ARQ) . . . , wherein the ARQ functions intermediate the application layer and a transport layer . . . to receive data packets for the application from the transport layer" and "scanning for the application . . . only the data packets accessed by the network intrusion detection process in a), . . . wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

The Present Office Action discounts Appellant's arguments presented above, which were also presented in Appellant's reply of January 21, 2009. Specifically, the Present Office Action responds that claim 25, "only passingly and broadly mentions . . . 'communication to an application receive queue.'" Applicant respectfully submits that this mischaracterizes the claim.

Further, Appellant pointed out specific language in the claim in the January 21, 2009, reply that relates to this matter. See above remarks and similar remarks in Appellant's reply of January 21, 2009, beginning at the end of page 11, which in addition to pointing out that claim 1 (and, correspondingly, independent claims 13 and 25) recites "communication to an application receive queue," also points out much more that the claim recites with regard to the ARQ. In particular, Appellant has pointed out the claim recites that the application receive queue ("ARQ") "functions intermediate the application layer and a transport layer." Appellant also pointed out that included in the ARQ functioning is functioning "to receive data packets for the application from the transport layer." Appellant also pointed out that the claimed method recites "scanning for the application . . . only the data packets accessed by the network intrusion detection process in a). " This makes clear that the claim limits the scanning to only data packets accessed by the network intrusion detection process in "communication to an application receive queue (ARQ) . . . intermediate the application layer and . . . transport layer . . . to receive data packets for the application from the transport layer." Still further, Appellant pointed out that the claim states "the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

Thus, Appellant respectfully disagrees with the assertion in the Present Office Action that the claim only passingly and broadly mentions "communication to an application receive queue," and submits that the Present Office Action essentially ignores the claim language recited above and Appellant's explanation thereof.

Further, the Present Office Action states "There Is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claims." Again, Appellant respectfully submits that this mischaracterizes the claim and ignores specific claim language about communication processed by a transport layer and then passed to an application receive queue between the transport layer and the application layer. That is, as Appellant has pointed out, the claim recites "scanning for the application . . . only the data packets accessed by the network

intrusion detection process in a). " This makes clear that the claim limits the scanning to only data packets accessed by the network intrusion detection process in "communication to an application receive queue (ARQ) . . . intermediate the application layer and . . . transport layer . . . to receive data packets for the application from the transport layer," since a) states "communication to an application receive queue (ARQ) . . . intermediate the application layer and . . . transport layer . . . to receive data packets for the application from the transport layer." Still further, Appellant pointed out that the claim limits the scanning to being "after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ."

The other art relied upon in the rejection does not cure the above deficiencies.

For all the above reasons, Appellant respectfully submits that claim 26 is patentably distinct.

Claim 26

Claim 26 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061). Appellant respectfully submits that the rejection is improper.

Examiner's Position

Appellant's arguments filed 1/21/09 have been fully considered but they are not persuasive. Appellant argues that Yadav fails to teach the "scanning of packets that have been processed by the transport layer and are on their way to a particular application queue receive" as mentioned in bottom of pg 11 of remarks. In reply, Appellant is reminded that the claim language is broad and is thus given its broadest reasonable interpretation. Since the claim only passingly and broadly mentions a "communication to an application receive queue" then this is treated broadly since the claim fails to limit whether this communication is destined to, belongs to, coming from, etc. in regards to the queue. There is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant's Rebuttal

The Present Office Action maintains the same prior art rejection stated in the previous Office action, which was dated October 17, 2008, and which asserted that Yadav column 5, lines 47-52, teaches tracking abnormally behaving applications. The previous Office action stated that "it is common knowledge that if an application is behaving abnormally, and that it is possible due to an intrusion, then that application should be terminated in order to prevent any harmful effects that may result from the intrusion" and that it would have been obvious for one of ordinary skill in the art to modify Yadav to include terminating the application responsive to determining a scanned data packet is malicious, in order to prevent any harmful

effects that may result from the intrusion. Appellant respectfully submits that this analysis is not relevant to the present invention, as claimed.

In the present case, intrusions are detected before data received from a remote host for an application has been passed to the application, and thus before the data can cause the application to behave abnormally by scanning data for an application in the manner recited in claim 25. See previous explanation on page 13 of Appellant's Response Accompanying Request for Continuing Examination, submitted August 4, 2008. Nevertheless, in one aspect of the present invention, as recited in claim 26 when read in connection with claim 25, an application is terminated responsive to detecting the malicious data packet. It logically follows from claims 25 and 26 of the present case that an application is terminated due to detecting an intrusion, but before the application can be subjected to any harmful effects of the intrusion and, therefore, before the application has an opportunity to behave abnormally. This does not follow from the logic presented in the previous Office action that posits reasons for terminating an application if the application is behaving abnormally due to an intrusion. Therefore, it would not be obvious to modify Yadav according to the logic put forward by the previous Office action (which is not further supplemented in the Present Office Action).

The other art relied upon in the rejection does not cure the above deficiencies.

Consequently, Appellant respectfully submits that claim 26 is patentably distinct.

Further, Appellant presented arguments contrary to the alleged common knowledge presented in the previous Office action and requested in the reply of January 21, 2009, in accordance with MPEP 2144.03(C), that Examiner submit an examiner's affidavit or declaration providing a basis for the alleged common knowledge if the rejection of claim 26 was maintained. However, the rejection was maintained but no examiner's affidavit or declaration has been provided by the Present Office Action. For this additional reason Appellant respectfully submits that claim 26 is patentably distinct.

Claim 37

Claim 37 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061). Appellant respectfully submits that the rejection is improper.

Examiner's Position

Appellant's arguments filed 1/21/09 have been fully considered but they are not persuasive. Appellant argues that Yadav fails to teach the "scanning of packets that have been processed by the transport layer and are on their way to a particular application queue receive" as mentioned in bottom of page 11 of remarks. In reply, Appellant is reminded that the claim language is broad and is thus given its broadest reasonable interpretation. Since the claim only passingly and broadly mentions a "communication to an application receive queue" then this is treated broadly since the claim fails to limit whether this communication is destined to, belongs to, coming from, etc. in regards to the queue. There is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant's Rebuttal

The Present Office Action maintains the same prior art rejection stated in the previous Office action, which was dated October 17, 2008, and which asserted that Yadav, column 6, lines 25-31, teaches intimating a transport layer to tear down a remote host connection responsive to determining a scanned data packet is malicious. Appellant respectfully disagrees. In this passage, Yadav teaches that "If an inbound communication 262 fails to correspond to an authorized request . . . the communication is dropped (i.e., blocked from passage to another layer . . ." Blocking communication from passing to another layer is not the same as, nor does it suggest, intimating the transport layer to tear down a remote host connection responsive to

determining a scanned data packet is malicious. Tearing down a connection typically includes invoking a "send disconnect" type function and also invoking a "close socket" type function, for example. See, for example, http://msdn.microsoft.com/en-us/library/ms737616(VS.85).aspx. This closes a channel of communication that existed between the application and the remote host via the network and does not merely block communication from passing to another layer in the target computer system.

The other art relied upon in the rejection does not cure the above deficiencies.

Consequently, Appellant respectfully submits that claim 37 is patentably distinct.

Claim 40

Claim 40 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061). Appellant respectfully submits that the rejection is improper.

Examiner's Position

Appellant's arguments filed 1/21/09 have been fully considered but they are not persuasive. Appellant argues that Yadav fails to teach the "scanning of packets that have been processed by the transport layer and are on their way to a particular application queue receive" as mentioned in bottom of page 11 of remarks. In reply, Appellant is reminded that the claim language is broad and is thus given its broadest reasonable interpretation. Since the claim only passingly and broadly mentions a "communication to an application receive queue" then this is treated broadly since the claim fails to limit whether this communication is destined to, belongs to, coming from, etc. in regards to the queue. There is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant's Rebuttal

The Present Office Action maintains the same prior art rejection stated in the previous Office action, which was dated October 17, 2008, and which asserted that Yadav, column 6, lines 25-31, teaches intimating a transport layer to tear down a remote host connection responsive to determining a scanned data packet is malicious. Appellant respectfully disagrees. In this passage, Yadav teaches that "If an inbound communication 262 fails to correspond to an authorized request . . . the communication is dropped (i.e., blocked from passage to another layer . . ." Blocking communication from passing to another layer is not the same as, nor does it suggest, intimating the transport layer to tear down a remote host connection responsive to

determining a scanned data packet is malicious. Tearing down a connection typically includes invoking a "send disconnect" type function and also invoking a "close socket" type function, for example. See, for example, http://msdn.microsoft.com/en-us/library/ms737616(VS.85).aspx. This closes a channel of communication that existed between the application and the remote host via the network and does not merely block communication from passing to another layer in the target computer system.

The other art relied upon in the rejection does not cure the above deficiencies.

Consequently, Appellant respectfully submits that Claim 40 is patentably distinct.

Claim 43

Claim 43 stands rejected under 35 U.S.C. 103(a) as being unpatentable over Yadav (US Patent No 7174566) in view of Holland (US Patent No 6,851,061). Appellant respectfully submits that the rejection is improper.

Examiner's Position

Appellant's arguments filed 1/21/09 have been fully considered but they are not persuasive. Appellant argues that Yadav fails to teach the "scanning of packets that have been processed by the transport layer and are on their way to a particular application queue receive" as mentioned in bottom of page 11 of remarks. In reply, Appellant is reminded that the claim language is broad and is thus given its broadest reasonable interpretation. Since the claim only passingly and broadly mentions a "communication to an application receive queue" then this is treated broadly since the claim fails to limit whether this communication is destined to, belongs to, coming from, etc. in regards to the queue. There is also nothing in the claim that limits the communication to being processed by a transport layer. Thus, it is noted that the features upon which Appellant relies are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See In re Van Geuns, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant's Rebuttal

The Present Office Action maintains the same prior art rejection stated in the previous Office action, which was dated October 17, 2008, and which asserted that Yadav, column 6, lines 25-31, teaches intimating a transport layer to tear down a remote host connection responsive to determining a scanned data packet is malicious. Appellant respectfully disagrees. In this passage, Yadav teaches that "If an inbound communication 262 fails to correspond to an authorized request . . . the communication is dropped (i.e., blocked from passage to another layer . . ." Blocking communication from passing to another layer is not the same as, nor does it suggest, intimating the transport layer to tear down a remote host connection responsive to

determining a scanned data packet is malicious. Tearing down a connection typically includes invoking a "send disconnect" type function and also invoking a "close socket" type function, for example. See, for example, http://msdn.microsoft.com/en-us/library/ms737616(VS.85).aspx. This closes a channel of communication that existed between the application and the remote host via the network and does not merely block communication from passing to another layer in the target computer system.

The other art relied upon in the rejection does not cure the above deficiencies.

Consequently, Appellant respectfully submits that Claim 43 is patentably distinct.

Claims 3-4, 7, 9-11, 15-16, 19-23, 27-28, 31, 33-34, 36, 38-39, 41-42, and 44

Claims 3-4, 7, 9-11, 15-16, 19-23, 27-28, 31, 33-34, 36, 38-39, 41-42, and 44 are allowable at least because they depend upon allowable base claims. Therefore, the rejection of claims 3-4, 7, 9-11, 15-16, 19-23, 27-28, 31, 33-34, 36, 38-39, 41-42, and 44 under 35 U.S.C. 103(a) is not proper.

REQUEST FOR ACTION

For the above reasons, Appellant requests that all the pending claims of the present application be allowed and that the application be promptly passed to issuance.

Respectfully submitted,

/anthony v.s. england/

Anthony V.S. England
Registration No. 35,129
Attorney of Record for
IBM Corporation
Telephone: 512-477-7165
a@aengland.com

Attachments: Claims Appendix, Evidence Appendix, Related Proceedings Appendix

APPENDIX "AA" CLAIMS

1. (previously presented) A method of detecting an intrusion in a communications network, the method comprising the steps of:

a) accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer;

b) scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process in a), wherein the data packets are directed to the application from a remote host via the communications network, and wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ;

c) determining if said scanned data packets are malicious; and

d) taking at least one action to prevent the application from processing data packets from the remote host to the application responsive to c) determining that any of the scanned data packets are malicious.

2. (previously presented) The method according to claim 1, wherein said at least one action includes terminating the application.

3. (original) The method according to claim 1, further comprising the step of transmitting to said application layer any data packets determined not to be malicious.

4. (original) The method according to claim 1, wherein said scanning and determining steps are implemented using a scan module.

APPENDIX "AA" CLAIMS

5-6. (canceled)

7. (previously presented) The method according to claim 1, further comprising the step of obtaining data from said at least one ARQ.

8. (canceled)

9. (original) The method according to claim 1, further comprising the step of dispatching said data packets to one or more handlers for scanning, if said protocol is monitored.

10. (original) The method according to claim 1, wherein said scanning and determining steps are implemented using a scan daemon.

11. (previously presented) The method according to claim 1, further comprising the step of the target computer system generating fake, network-accessible services.

12. (withdrawn) A method of preventing an intrusion in a communications network, the method comprising the steps of:

disabling a network interface of a host if an idle time expires;

determining if any packets are to be transmitted; and

enabling said network interface if at least one packet is determined to be available to be transmitted.

APPENDIX "AA" CLAIMS

13. (previously presented) A target computer system for detecting an intrusion originating from a remote host and communicated to the target computer system via a communications network, the target computer system comprising:

a storage unit for storing data and instructions for a processing unit; and

a processing unit coupled to said storage unit, said processing unit being programmed to perform steps responsive to the instructions, wherein the steps comprise:

a) accessing, by a network intrusion detection process of the target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer;

b) scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process in a), wherein the data packets are directed to the application from the remote host via the communications network, and wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ;

c) determining if said scanned data packets are malicious; and

d) taking at least one action to prevent the application from processing the data packets from the remote host to the application responsive to c) determining that any of the scanned data packets are malicious.

14. (previously presented) The system according to claim 13, wherein said at least one action includes terminating the application.

APPENDIX "AA" CLAIMS

15. (original) The system according to claim 13, wherein said processing unit is programmed to transmit to said application layer any data packets determined not to be malicious.

16. (original) The system according to claim 13, wherein said processing unit is programmed to implement a scan module.

17-18. (canceled)

19. (previously presented) The system according to claim 13, wherein said processing unit is programmed to obtain data from said at least one ARQ.

20. (previously presented) The system according to claim 13, wherein said scanning is performed on data packets from said at least one ARQ.

21. (original) The system according to claim 13, wherein said processing unit is programmed to dispatch said data packets to one or more handlers for scanning, if said protocol is monitored.

22. (original) The system according to claim 13, wherein said scanning and determining are implemented using a scan daemon.

23. (previously presented) The system according to claim 13, wherein said processing unit is programmed to generate fake, network-accessible services.

24. (withdrawn) A system of preventing an intrusion in a communications network, the system comprising:

a storage unit for storing data and instructions for a processing unit; and

APPENDIX "AA" CLAIMS

a processing unit coupled to said storage unit, said processing unit being programmed to disable a network interface of a host if an idle time expires, to determine if any packets are to be transmitted, and to enable said network interface if at least one packet is determined to be available to be transmitted.

25. (previously presented) A computer program product stored on a computer-readable storage medium, the computer program product having instructions for execution by a computer, wherein the instructions, when executed by the computer, cause the computer to implement a method comprising the steps of:

a) accessing, by a network intrusion detection process of a target computer system, communication to an application receive queue (ARQ) for an application running in an application layer of the target computer system, wherein the ARQ functions intermediate the application layer and a transport layer of a network protocol associated with said communications network to receive data packets for the application from the transport layer;

b) scanning for the application by the network intrusion detection process only the data packets accessed by the network intrusion detection process in a), wherein the data packets are directed to the application from a remote host via the communications network, and wherein the scanning is after the data packets have been processed by the transport layer and after the transport layer has passed the processed data packets for receipt by the application's ARQ;

c) determining if said scanned data packets are malicious; and

d) taking at least one action to prevent the application from processing data packets from the remote host to the application responsive to c) determining that any of the scanned data packets are malicious.

APPENDIX "AA" CLAIMS

26. (previously presented) The computer program product according to claim 25, wherein said at least one action includes terminating the application.

27. (previously presented) The computer program product according to claim 25, the steps further comprising transmitting to said application layer any data packets determined not to be malicious.

28. (previously presented) The computer program product according to claim 25, wherein said scanning and determining are implemented using a scan module.

29-30. (canceled)

31. (previously presented) The computer program product according to claim 25, the steps further comprising obtaining data from said at least one ARQ.

32. (canceled)

33. (previously presented) The computer program product according to claim 25, the steps further comprising dispatching said data packets to one or more handlers for scanning, if said protocol is monitored.

34. (previously presented) The computer program product according to claim 25, wherein said scanning and determining are implemented using a scan daemon.

35. (withdrawn) A computer-readable medium of preventing an intrusion in a communications network, the computer-readable medium comprising:

programmed instructions for disabling a network interface of a host if an idle time expires;

APPENDIX "AA" CLAIMS

programmed instructions for determining if any packets are to be transmitted; and

programmed instructions for enabling said network interface if at least one packet is determined to be available to be transmitted.

36. (previously presented) The method according to claim 1, wherein said at least one action includes modifying firewall rules to prevent reception of data packets from the host computer system.

37. (previously presented) The method according to claim 1, wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and wherein said at least one action includes intimating the transport layer to tear down the remote host connection.

38. (previously presented) The method according to claim 37, wherein after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection.

39. (previously presented) The system according to claim 13, wherein said at least one action includes modifying firewall rules to prevent reception of data packets from the host computer system.

40. (previously presented) The system according to claim 13, wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and wherein said at least one action includes intimating the transport layer to tear down the remote host connection.

APPENDIX "AA" CLAIMS

41. (previously presented) The system according to claim 40, wherein after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection.

42. (previously presented) The computer program product according to claim 25, wherein said at least one action includes modifying firewall rules to prevent reception of data packets from the host computer system.

43. (previously presented) The computer program product according to claim 25, wherein the directing of the data packets to the application from the remote host is via a connection with the remote host on the communications network, and wherein said at least one action includes intimating the transport layer to tear down the remote host connection.

44. (previously presented) The computer program product according to claim 43, wherein after intimating the transport layer to tear down the remote host connection, the target computer services requests on connections other than that remote host connection.

APPENDIX "BB" EVIDENCE

NONE.

APPENDIX "CC" RELATED PROCEEDINGS

NONE.